UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KLAUS BIESENBACH,

Plaintiff,

v.

JOHN DOES 1-3,

Defendant.

Case No. 21-cv-08091-DMR

ORDER GRANTING IFP APPLICATION AND SCREENING COMPLAINT PURSUANT TO 28 U.S.C. § 1915(E)

Re: Dkt. Nos. 1, 2, 5

Plaintiff Klaus Biesenbach filed a complaint ("Compl.") and an application for leave to proceed *in forma pauperis* ("IFP"). [Docket Nos. 1, 2.] He also filed an ex parte application for expedited discovery. [Docket No. 5.] Having considered Biesenbach's papers, the court grants the IFP application but finds that the complaint fails to state a claim on which relief may be granted pursuant to 28 U.S.C. § 1915(e). In light of this ruling, the court further denies Biesenbach's application for expedited discovery without prejudice. Plaintiff may file a first amended complaint that addresses the deficiencies identified in this screening order within twenty-one days—i.e., by **February 14, 2022**.[1]

I. BACKGROUND

Biesenbach, a resident of San Francisco, claims that he was the victim of multiple cyber hacking incidents by three anonymous Doe Defendants ("Defendants"). He avers that "each

[1] Biesenbach has also filed multiple documents without support or explanation that appear to be ISP, Google Workspace, and computer system logs—many of which the clerk has stricken as improperly filed. [Dockets Nos. 11, 12, 17, 18.] The court will not entertain further filings of stand-alone exhibits without providing any justification or explanation to the court of their relevance. All future such filings must be attached to Biesenbach's first amended complaint and/or to a sworn affidavit that authenticates them—that is, lays foundational evidence establishing Biesenbach's personal knowledge of these logs, what they are, how he came to retrieve them. *See* Fed. R. Evid. 901(a) ("To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.").

Defendant has been seen with a person who Plaintiff has had an incident with before and has his phone number." Compl. ¶ 5. Biesenbach determined that Defendants are located in this judicial district through geolocation of their Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, and Android device identification number, as well as "having been approached" by them. *Id.* Biesenbach says that because of their "persistent observed activity," they are not "transitory or occasional" residents of this district. *Id.*

On April 18, 2021 Biesenbach subscribed to G-Suite Business Plus, a collection of cloud computing products developed by Google, and registered a domain name "Targetedindividualsresource.org." *Id.* ¶ 7. G-Suite allows for Mobile Device Management, a security software that allows IT departments to implement policies that secure, monitor, and manage end-user mobile devices. *Id.* Biesenbach says that this software helps secure networks while allowing users to use their own devices; through it, administrators can monitor if third-party mobile devices have accessed the software user's data. *Id.*

Biesenbach alleges that on April 21, 2021, Defendants monitored his cellphone communications and multiple encrypted WiFi networks without authorization. Compl. ¶ 8. Defendants then used multiple log-in credentials to access Biesenbach's G-Suite account using a particular Android device; Biesenbach recorded the unique identification number for the device. *Id.* Between April 21 and September 1, 2021, Defendants accessed Biesenbach's account and bypassed Google's security authentication process. *Id.* ¶ 10. He claims that they used a program to alter their Android device's unique identifiers. *Id.*

Around May 23, 2021, Biesenbach generated an "IT admin report"[2] showing "two devices using one email address"—presumably those that he alleges accessed his account without authorization. *Id.* ¶ 11. Biesenbach immediately notified "California Elections" of a breach to his voter file and Google's G-Suite Support team. *Id.* The Google team "did not provide [him] assistance with identifying the Google Android user" and instead directed him to their legal department; Biesenbach does not say if he received any response regarding his voter file

[2] The court does not know what such a report is or how it is generated.

complaint. *Id.*

Biesenbach claims other incidents of unauthorized access to his G-suite account. Around July 20, 2021, Biesenbach tried to register for Google's Voice-over-Internet-Protocol ("VOIP") telephone service, but Defendants allegedly prevented his access by "changing the passwords and denying [him] the ability to audit and view stored information sent by phone, texts, [and] emails." Compl. ¶ 12. Around August 7, 2021, Biesenbach received a call from a phone number that his audit logs later were "changed to anonymous," which he asserts was an "alteration of a record stored . . . offsite." *Id.* ¶ 13. On August 8, 2021, Biesenbach claims that Defendants told him they were members of the Carrillo Cartel from Guadalajara, Mexico—although he does not explain how they communicated with him. *Id.* ¶ 14. Defendants "threatened [him] and demanded [him] to turn over his computer." *Id.* Biesenbach said he recognized that one of the individuals who contacted him was someone he met three years ago named "Manny." *Id.* On August 9, 2021, Defendants allegedly accessed Biesenbach's WiFi and changed his password, which prevented him from accessing his router on multiple occasions. *Id.* ¶ 15.

Biesenbach alleges five claims under various federal statutes prohibiting cyberstalking, wiretapping, and computer fraud. He seeks $2.8 million in damages and a "judgement that the claims . . . were done with the intent to cause irreparable harm." Compl. ¶ 21.

II. LEGAL STANDARD

A court may allow a plaintiff to prosecute an action in federal court without prepayment of fees or security if the plaintiff submits an affidavit showing that he or she is unable to pay such fees or provide such security. *See* 28 U.S.C. § 1915(a). A court is under a continuing duty, however, to dismiss a case filed without the payment of the filing fee whenever it determines that the action "(i) is frivolous or malicious; (ii) fails to state a claim on which relief may be granted; or (iii) seeks monetary relief against a defendant who is immune from such relief." 28 U.S.C. § 1915(e)(2)(B)(i)-(iii). If the court dismisses a case pursuant to 28 U.S.C. § 1915(e)(2)(B), the plaintiff may still file the same complaint by paying the filing fee. This is because the court's section 1915(e)(2)(B) dismissal is not on the merits, but rather an exercise of the court's discretion under the IFP statute. *Denton v. Hernandez*, 504 U.S. 25, 32 (1992).

To make the determination under 28 U.S.C. § 1915(e)(2)(B), courts assess whether there is an arguable factual and legal basis for the asserted wrong, "however inartfully pleaded." *Franklin v. Murphy*, 745 F.2d 1221, 1227-28 (9th Cir. 1984). Courts have the authority to dismiss complaints founded on "wholly fanciful" factual allegations for lack of subject matter jurisdiction. *Id.* at 1228. A court can also dismiss a complaint where it is based solely on conclusory statements, naked assertions without any factual basis, or allegations that are not plausible on their face. *Ashcroft v. Iqbal*, 556 U.S. 662, 677-78 (2009); *see also Erickson v. Pardus*, 551 U.S. 89, 93-94 (2007) (per curiam). Dismissal is proper where "no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory." *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010). A claim has facial plausibility when a plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 677-78.

Although pro se pleadings are liberally construed and held to a less stringent standard than those drafted by lawyers, *see Erickson*, 551 U.S. at 94, a complaint, or portion thereof, should be dismissed for failure to state a claim if it fails to set forth "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554 (2007); *see also* Fed. R. Civ. P. 12(b)(6). "[A] district court should not dismiss a pro se complaint without leave to amend unless it is absolutely clear that the deficiencies of the complaint could not be cured by amendment." *Akhtar v. Mesa*, 698 F.3d 1202, 1212 (9th Cir. 2012).

III. 28 U.S.C. § 1915(E) SCREENING

Having evaluated Biesenbach's financial affidavit, the court finds that he has satisfied the economic eligibility requirement of 28 U.S.C. § 1915(a) and grants the application to proceed IFP. The court's grant of Biesenbach's application to proceed IFP, however, does not mean that he may continue to prosecute the complaint.

Biesenbach's complaint is unclear and hard to follow. It contains citations to various laws. *See* Compl. ¶¶ 16-21. Liberally construed, the complaint appears to allege violations of laws prohibiting interstate stalking and domestic violence, 18 U.S.C. § 2261A; the Wiretap Act, 18 U.S.C. §§ 2511, 2520; the Secured Communications Act, 18 U.S.C. § 2701(a)(1), and the

Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5). None of Biesenbach's allegations, however, state a cognizable legal claim.

A. Cyberstalking

First, Biesenbach alleges a violation of 22 U.S.C. § 2266(2). *See* Compl. ¶ 16. That provision simply sets forth the definition of "Course of conduct" as used in the relevant code chapter as "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose." As the definitions section alone does not create a legal violation, the court liberally construes Biesenbach's claim as arising under the relevant statute, 22 U.S.C. § 2261A. That law creates a federal criminal offense for cyberstalking, including "harassing and intimidating conduct." *See United States v. Osinger*, 753 F.3d 939, 944 (9th Cir. 2014). "Case law is . . . unanimous that no private right of action is available under § 2261A." *Cain v. Christine Valmy Int'l Sch.*, 216 F. Supp. 3d 328, 335 (S.D.N.Y. 2016) (citing cases); *accord Kruska v. Perverted Justice Foundation, Inc.*, No. 08-cv-0054, 2009 WL 321146, at *4 (D. Ariz. Feb. 6, 2009) ("The act creates no private right of recovery."). Rather, the law is a "bare criminal statute[.]" *Cain*, 216 F. Supp. 3d at 335. Because 22 U.S.C. § 2261A does not create a civil offense, this allegation does not state a claim for relief.

B. Wiretap Act

Second, Biesenbach alleges claims under the Wiretap Act, 18 U.S.C. §§ 2511(1)(d), 2520(a). Compl. ¶ 17, 20.[3] "The Wiretap Act prohibits the unauthorized 'interception' of an 'electronic communication.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis*, 141 S. Ct. 1684 (2021) (quoting 18 U.S.C. § 2511(1)(a)-(e)). 18 U.S.C. § 2511(1)(d) imposes liability against anyone who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication." Although § 2511 is a criminal provision, "[t]he civil damages provision of the federal [W]iretap [A]ct . . . provides a private right

[3] Biesenbach mis-cites to "18 U.S.C. § 2511(d)" but quotes (albeit with alterations) a portion of 18 U.S.C. § 2511(1)(d) in his allegation.

of action to 'any person whose wire . . . communication is intercepted, disclosed, or intentionally used in violation of this chapter.'" *Noel v. Hall*, 568 F.3d 743, 747 (9th Cir. 2009) (quoting 18 U.S.C. § 2520) (second alteration in original)); *Dish Network L.L.C. v. Gonzalez*, No. 1:13-CV-00107-LJO, 2013 WL 2991040, at *3 (E.D. Cal. June 14, 2013) ("Although Section 2511 is a criminal provision which does not itself provide a private right of action, 18 U.S.C. § 2520(a) does provide a private cause of action" (quotations omitted)). "[A] plaintiff may bring a civil action under § 2520 whether or not the defendant had been subject to criminal prosecution and conviction." *DIRECTV, Inc. v. EQ Stuff, Inc.*, 207 F. Supp. 2d 1077, 1084 (C.D. Cal. 2002) (quotation omitted). The court therefore construes Biesenbach's complaint as alleging civil liability against Defendants for a violation of 18 U.S.C. § 2511(1)(d).

"The Wiretap Act defines 'intercept' to mean 'the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.'" *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1005 (N.D. Cal. 2017) (quoting 18 U.S.C. § 2510(4)). "The term 'acquisition' is not defined in the statute, but the Ninth Circuit, looking at the term's 'ordinary meaning' has defined it as the 'act of acquiring, or coming into possession of.'" *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015) (quoting *United States v. Smith*, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998)). "It has further held that 'such acquisition occurs when the contents of a wire communication are captured or redirected in any way.'" *Id.* (quoting *Noel*, 568 F.3d at 749).

Also, the Wiretap Act defines "contents" as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The Ninth Circuit has held that "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). While communications such as text messages and URLs containing search terms constitute protected "contents," user names, contact information, geographic information, PIN numbers, and passwords do not. *Carrier*, 78 F. Supp. 3d at 1082-83 (surveying cases).

Although Biesenbach alleged facts that Defendants hacked into his G-Suite accounts, cell

phone, WiFi, and router, he has not plausibly pleaded any of the elements necessary for a Wiretap Act claim. First, Biesenbach only alleges that Defendants accessed his accounts or devices. *See, e.g.*, Compl. ¶¶ 8, 10, 15. He fails to allege that Defendants *acquired*, i.e., captured or redirected, the contents of any communications in those accounts or devices. Nor did he plead that Defendants actually used those communications for any purpose. *See Satchell*, 234 F. Supp. 3d at 1008-09 (dismissing allegations under 18 U.S.C. § 2511(1)(d) against smartphone application developers where no facts alleged "to show that the contents of [plaintiff's] communications . . . were used to send her targeted advertising.").

Relatedly, Biesenbach fails to allege that Defendants intercepted particular "contents" of his communications that are protected under the Wiretap Act. His complaint only refers to incidents in which Defendants accessed his accounts "chang[ed] the passwords" to his G-Suite and Wifi without authorization. *See* Compl. ¶¶ 12, 15; *Carrier*, 78 F. Supp. 3d at 1084 (while passwords are "may be a prerequisite to engaging in communications . . . the credentials themselves do not reveal the substance, purport, or meaning of any communication"). Biesenbach does not describe if Defendants in fact seized any of his actual communications, such as emails or text messages. Accordingly, Biesenbach failed to state a claim under 18 U.S.C. § 2511(1)(d).

C. Stored Communications Act

Third, Biesenbach alleges violations of the Stored Communications Act ("SCA"), 18 U.S.C § 2701(a)(1). The SCA "covers access to electronic information stored in third party computers." *Zynga*, 750 F.3d at 1104. "The [SCA] provides a private right of action against anyone who: '(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) initially exceeds an authorization to access that facility . . . while it is in electronic storage in such system.'" *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 685 (N.D. Cal. 2021) (quoting 18 U.S.C. § 2701(a)). A plaintiff must plead that the defendant "(1) gained unauthorized access to a 'facility' where it (2) accessed an electronic communication in 'electronic storage.'" *Facebook*, 956 F.3d at 608.

The SCA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12); *see id.* § 2711(1). The SCA further defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17)).

"The SCA does not provide a statutory definition of facility." *Calhoun v. Google, LLC*, 546 F. Supp. 3d 605, 626 (N.D. Cal. 2021); *see Facebook*, 956 F.3d at 609 n.10 (declining to address whether personal computers, web browsers, and browser managed files are "facilities"). However, multiple circuit and district courts, including in this district, have ruled that "a user's personal device is not a facility under the SCA." *Calhoun*, 546 F. Supp. 3d at 628; *see, e.g., id.* (Google's Chrome web browser not a covered facility); *Lopez*, 519 F. Supp. 3d at 686 (Apple's Siri software not covered); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 822 (N.D. Cal. 2020) (Google Assistant Enabled devices not covered); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012) (Apple iPhone not covered). "Ultimately, the SCA is meant to protect information held by centralized communication providers[; it] is not meant to provide a catch-all to protect the privacy of stored internet communications." *Lopez*, 519 F. Supp. 3d at 686 (internal citations omitted); *see also Facebook*, 956 F.3d at 609 ("[T]he SCA has typically only been found to apply in cases involving a centralized data-management entity; for instance, to protect servers that stored emails for significant periods of time between their being sent and their recipients' reading them.").

Biesenbach claims that "Defendants used log-in credentials with the intent to bypass G Suites[']s security software gaining access to plaintiff's organizational data hosted on a server." Compl. ¶ 18. He claims he has a right to damages because he is a "licensee of Google's VOIP telephone service." *Id.*[4] Biesenbach's SCA allegation fails for three reasons. First, Biesenbach does not explain what he refers to as his "organizational data." Without more detail, the court

[4] Biesenbach does not explain why his VOIP license is relevant here.

cannot conclude that this data plausibly constitutes protected "electronic communications" within the Act. Second, Biesenbach refers to his VOIP service in this claim and to his G-Suite Account, cell phone, WiFi, and router elsewhere in the complaint. He has not plausibly alleged, however, that these accounts or devices constitute protected "facilities." At least three of the devices—his cell phone, WiFi, and router—are or are likely to be the types of personal devices that other courts have held fall outside the purview of the SCA. While information on his G-Suite Account that is allegedly "hosted on a server," Compl. ¶ 18, may fall within electronic storage in third-party facilities, Biesenbach has not fully described the nature of the communications, the server in question, and why it falls within the purview of "electronic storage," *see Facebook*, 956 F.3d at 609; *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (holding that e-mail messages held on an ISP's server were in electronic storage). Absent further factual allegations, Biesenbach does not plausibly state a SCA claim.

D. Computer Fraud and Abuse Act

Finally, Biesenbach alleges claims under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A), (C). Compl. ¶¶ 18-19.[5] 18 U.S.C. § 1030(a)(5)(A) establishes criminal liability for anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." Section 1030(a)(5)(C) also establishes criminal liability for anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."

"The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009). A protected computer is defined as "'an electronic. . . or other high speed data processing device

[5] Again, Biesenbach mis-cites to "18 U.S.C. § 1030(a)(2)(C)" but quotes § 1030(a)(5)(A) in his allegation. He also mis-cites to 18 U.S.C. § 1030(a)(5)(A) but quotes § 1030(a)(5)(C). Based on his quoted text, the court presumes that he alleges violations of § 1030(a)(5)(A) and (C).

performing logical, arithmetic, or storage functions' that 'is used in or affecting interstate or foreign commerce or communication.'" *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 451 (N.D. Cal. 2018) (quoting 18 U.S.C. § 1030(e)(1)-(2)) (holding cellular phones are protected). "This definition captures any device that makes use of a[n] electronic data processor, examples of which are legion." *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011)

Plaintiffs may file a civil action for damages and equitable relief violations of the CFAA pursuant to 18 U.S.C. § 1030(g). *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021); *LVRC Holdings*, 581 F.3d at 1132. Section 1030(g) section provides:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).

"Thus, a private plaintiff must prove that the defendant violated one of the provisions of § 1030(a)(1)-(7), and that the violation involved one of the factors listed in § 1030[(c)(4)(A)(i)]." *LVRC Holdings*, 581 F.3d at 1132. Those factors are:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
> (III) physical injury to any person;
> (IV) a threat to public health or safety; or
> (V) damage affecting a computer system used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security[.]

18 U.S.C. § 1030(c)(4)(A)(i).

The CFAA defines a "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting 18 U.S.C. § 1030(e)(11)).

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Thus, while 'damage' covers harm to data and information, 'loss' refers to monetary harms sustained by the plaintiff." *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 961 (N.D. Cal. 2014). The Ninth Circuit has held that the statute maintains a "narrow conception of 'loss,'" and that its definition, "with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself." *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262-63 (9th Cir. 2019). "[A]ny theory of loss must conform to the limited parameters of the CFAA's definition." *Id.* at 1263.

Biesenbach plausibly alleged that Defendants accessed his cell phone, WiFi network, and router without authorization in contravention of 18 U.S.C. § 1030(a)(5)(C). Compl. ¶¶ 8, 15. Biesenbach also appears to have plausibly alleged that Defendants "caused the transmission of a program . . . or command" that resulted in changing his passwords and access to his VOIP and router in contravention of § 1030(a)(5)(A). Compl. ¶¶ 12, 15. However, Biesenbach does not plead any that he suffered a monetary loss or damage of at least $5,000 as required under § 1030(c)(4)(A)(i)(I).[6] He does not, for instance, plead that he incurred any costs in responding to Defendants' alleged hacking or that he lost income or revenue because of an interruption in access to his accounts. *See Andrews*, 932 F.3d at 1263 (holding that plaintiff lacked cognizable injury under CFAA where he "does not—and cannot—argue that his allegedly lost revenue occurred because of an interruption of service.") Biesenbach's conclusory request for an award of $2.8 million is insufficient given the CFAA's narrow definition of loss. Accordingly, the complaint fails to state a claim under the CFAA.

IV. EX PARTE APPLICATION FOR EARLY DISCOVERY

Biesenbach also filed an *ex parte* application for early discovery to identify the identities of the three Doe Defendants. [Docket No. 5.] In the Ninth Circuit, "exceptions to the general rule" that discovery may not be initiated prior to the Federal Rule of Civil Procedure 26(f) conference

[6] None of the other factors appear relevant here.

are "generally disfavored." *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 577 (N.D. Cal. 1999) (citing *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). However, a court may authorize earlier discovery "for the parties' and witnesses' convenience and in the interests of justice." Fed. R. Civ. P. 26(d)(3). Courts have permitted "limited discovery . . . after [the] filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant." *Columbia*, 185 F.R.D. at 577. The plaintiff must show good cause for early discovery. *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002). "Good cause may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *Id.*

In evaluating whether a plaintiff establishes good cause to learn the identity of Doe defendants through early discovery, courts employ safeguards to ensure that such discovery "will only be employed in cases where the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service, and will prevent use of [early discovery] to harass or intimidate." *Columbia*, 185 F.R.D. at 578. Courts examine whether the plaintiff (1) has "identif[ied] the missing party with sufficient specificity such that the Court can determine that the defendant is a real person or entity who can be sued in federal court," (2) recounted "all previous steps taken to locate the elusive defendant," (3) established that the action can withstand a motion to dismiss, and (4) demonstrated a "reasonable likelihood that the discovery process will lead to identifying information about [the] defendant that would make service of process possible." *Id.* at 578-80. "Generally, ex parte applications for early discovery are accompanied by declarations which explain the party's efforts to determine the individual's identity and why the plaintiff believes that subpoenas to particular service providers would yield information regarding a defendant's identity." *Bellwether Coffee Co. v. Does 1-5*, No. 21-03612-JSC, 2021 WL 2333848, at *1 (N.D. Cal. June 8, 2021); *see Columbia*, 185 F.R.D. at 580 (calling for "a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served").

In light of the court's ruling that Biesenbach's complaint could not withstand a motion to dismiss, Biesenbach's *ex parte* application for early discovery is denied without prejudice. The

court also notes that Biesenbach's application fails to satisfy the other required *Columbia* factors, including facts recounting his previous attempts to identify Defendants, and why his requested discovery is likely to lead to identification of Defendants.

V. CONCLUSION

For the reasons above, the court grants Biesenbach's application to proceed IFP but finds that the complaint fails to state a claim pursuant to 28 U.S.C. § 1915(e). Biesenbach must file a first amended complaint addressing the deficiencies identified in this order within 21 days—i.e., by **February 14, 2022**. If he does not file a timely first amended complaint, the court will recommend dismissal of his action.

Should Biesenbach also seek leave again to take early discovery, he must include a sworn declaration sworn under penalty of perjury establishing facts to support arguments for each *Columbia* element. As discussed above, Biesenbach also must not file documents without properly authenticating them and establishing their relevance. Finally, Biesenbach is instructed not to contact the court regarding the status of his case.

The court refers Biesenbach to the section "Representing Yourself" on the Court's website, located at https://cand.uscourts.gov/pro-se-litigants/, as well as the Court's Legal Help Centers for unrepresented parties. Parties may schedule an appointment by calling 415-782-8982 or emailing fedpro@sfbar.org.

IT IS SO ORDERED.

Dated: January 24, 2022

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
IT IS SO ORDERED

Donna M. Ryu
United States Magistrate Judge

United States District Court
Northern District of California